(19) (11) Publication number: **11120141**

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: **09285768**

(22) Application date: **17.10.97**

(51) Intl. Cl.: **G06F 15/00** G06F 13/00

(30) Priority:

(43) Date of application publication: **30.04.99**

(84) Designated contracting states:

(71) Applicant: **FUJITSU LTD**

(72) Inventor: **MOROOKA TOSHIHARU**
MATSUSHIMA TAKASHI
YANO SHINJI

(74) Representative:

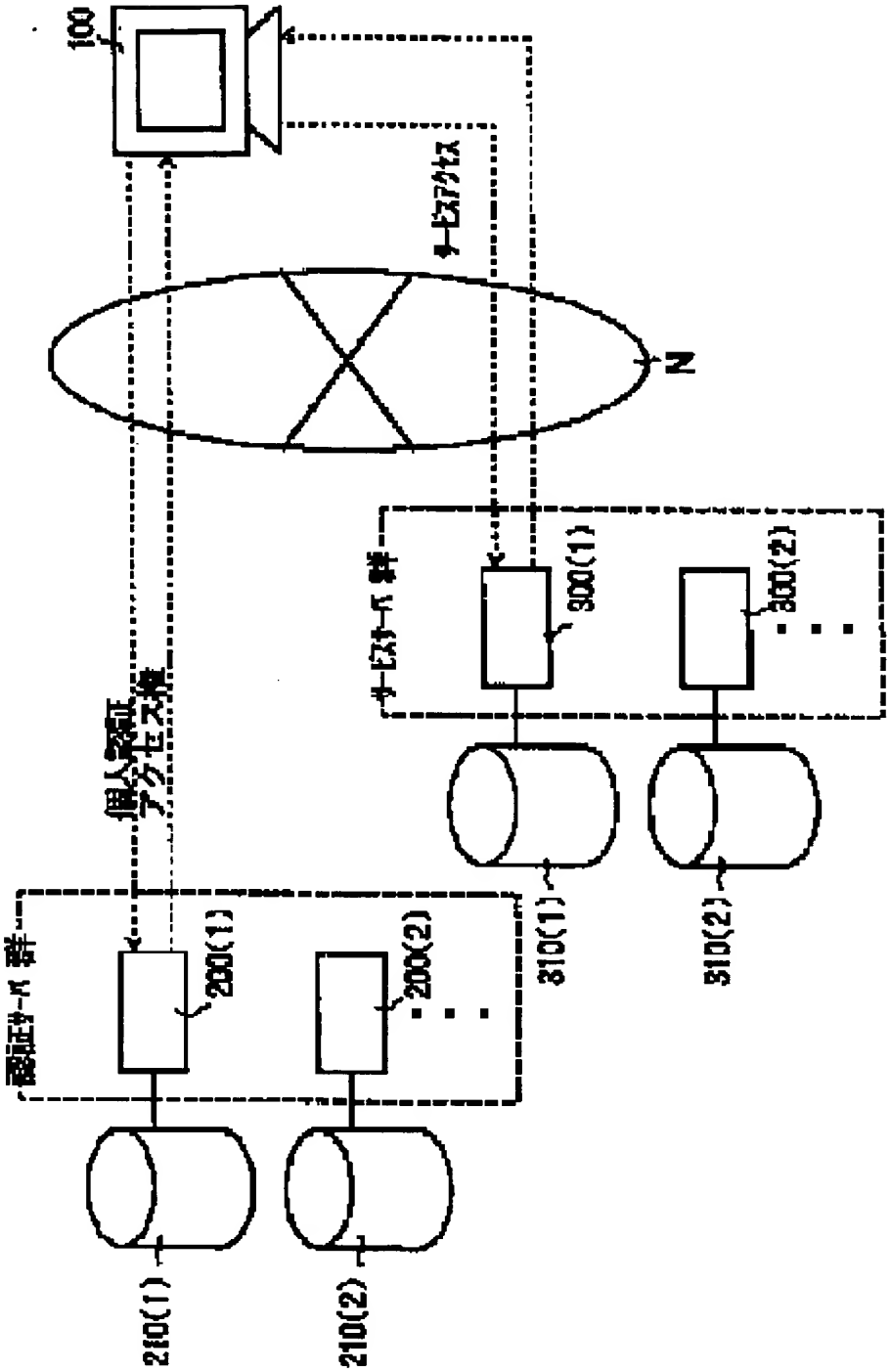
(54) DISTRIBUTED INFORMATION PROCESSING SYSTEM, AUTHENTICATION SYSTEM USED FOR THE SYSTEM AND SERVICE PROVISION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent loads of a processing from being concentrated to one station by transmitting permission information to a user terminal at the time of judging that information for permitting service provision included in authentication information is correct and then providing a service from a service provision system to the user terminal.

SOLUTION: User management files 210 (1) and 210(2) are connected to respective authentication servers 200 (1) and 200(2) and the respective user management files 210(1) and 210(2) preserve the information relating to the user of the user terminal connectable to the corresponding authentication server. Then, the respective authentication servers 200(1) and 200 (2) perform user authentication for an authentication request from the user terminal 100 through a network N, and when judged that the information for permitting the service provision included in the authentication is correct, transmit the permission information of the service provision to the user terminal 100 and thereafter, the service is provided from respective service

servers 300(1) and 300(2) to the user terminal 100.



Citation B

Japanese Patent Application Public-disclosure No. 11-120141
Japanese Patent Application Public-disclosure date: April 30, 1999
Japanese Patent Application No. 9-285768
Japanese Patent Application date: October 17, 1997
Title of the invention: Distributed information processing system and authentication system and service providing system used for the distributed information processing system
Gist of the invention:
[Industrial field of the invention]

The present invention is directed to a distributed information processing system consisting of a plurality of systems connected to one another via a network and in particular to a distributed information processing system where service is provided to an authenticated user terminal via a network. The present invention is further directed to an authentication system and service providing system used for a distributed information processing system such as described above.

[Embodiment]

Hereafter, an embodiment of the present invention is specifically described with reference to the attached drawings. Fig. 1 illustrates an example of a configuration of a distributed information processing system in accordance with an embodiment of the present invention. In Fig. 1, user terminal 100 is connected to network N (for example, the Internet), to which a plurality of authentication servers 200 (1), 200 (2), ... (authentication servers) and a plurality of service servers 300 (1), 300 (2), ... (service servers) are also connected. The authentication servers 200 (1), 200 (2), ... and service servers 300 (1), 300 (2), ... are respectively comprised of a common computer system. The service servers 300 (1), 300 (2), ... function as a database server in which information about service to be provided is stored. The user terminal 100 is comprised of a personal computer system and the like. Computer systems constituting authentication servers 200 (1), 200 (2), ..., service servers 300 (1), 300 (2), ... and user terminal 100 perform processing following the procedure described later in accordance with a program provided by a recording medium such as a CD-ROM or the like.

The authentication servers 200 (1), 200 (2), ... are coupled to user control files 210 (1), 210 (2), ... respectively. The user control files 210 (1), 210 (2), ... store information (user ID, user password or the like) about a user of a user terminal to which their corresponding authentication servers 200 (1), 200 (2), ... can be connected. In response to an authentication request from the user terminal 100 via the network N, the authentication servers 200 (1), 200 (2), ... conduct user authentication referring to the information in the corresponding user control files 210 (1), 210 (2), ...

The service servers 300 (1), 300 (2), ... are coupled to the authentication server control files 310 (1), 310 (2), ... respectively. The authentication server control files 310 (1), 310 (2), ... store information (authentication server ID, authentication server password and the like) about authentication servers accessible by their corresponding service servers 300 (1), 300 (2), ... The service servers 300 (1), 300 (2), ... provide service (information) in response to a service access from the user terminal 100 via network N.

Processing performed in a system such as described above follows the procedure indicated in Fig. 2. The user terminal 100 is provided with an authentication unit for performing processing concerning authentication and with a browser for conducting Internet communication. For simplicity's sake, an authentication server, a service server, a user control file and an authentication server control file are denoted by referential numerals 200, 300, 210 and 310 respectively in Fig. 2.

In Fig. 2, when a user inputs to the user terminal 100 a request for access to the authentication server (server resource) using an input unit (1), the browser sends the access request to the target authentication server 200 via Internet (2). In response to the access request, the authentication server 200 sends back the authorization information to the authorization information received by the browser is provided to the authentication unit (4). At this time, an input screen where a user ID (U-ID) and a password (U-PW) are entered is shown on, for example, a display screen of the user terminal 100.

When a user inputs the user ID (U-ID) and password (U-PW) to the user terminal 100 using the input unit (5), the authentication unit outputs an authentication request containing information about the user ID and password (6) and the authentication request is further transmitted from the

browser to the authentication server 200 (7). Upon receiving the authentication request, the authentication server 200 refers to the user control file 210 (8) and performs user authentication processing (9). The user authentication processing is performed following, for example, the procedure described in Fig. 3.

In Fig. 3, the user control file 210 is searched using as a key the user ID (U-ID) and password (U-PW) contained in the received authentication request (S1). Then, it is determined whether or not the user specified by the user ID (U-ID) and password (U-PW) is registered in the authentication server 200 or not (S2).

If it turns out that the user is registered, the authentication server ID (A-ID) and authentication service password (A-PW) for identifying the authentication server, the received user ID (U-ID) and access right are all encrypted using the authentication password (A-PW) (S3). In this context, an access right is information representing the contents of service, i.e., information about a type of service, the duration and number of times that the service is provided and the like.

Then, encrypted information including an access right described above and authentication server ID (A-ID) that is not encrypted are issued as authentication information from the authentication server 200 (S4). On the other hand, if the user identified by the user ID (U-ID) and password (U-PW) is not registered in the authentication server 200 (when at least one of the entered user ID and password is wrong) (S2, NG), the authentication server 200 issues a message to the effect that the user cannot be authenticated (NG) (S5).

Going back to Fig. 2, when the authentication server 200 issues authentication information as described above, the authentication information is transmitted to the user terminal 100 via the Internet (network N) (10). When the authentication unit in the user terminal 100 receives authentication information via the browser, the authentication information is held in the internal memory (11). In this state, an authorization message authorizing a service access is displayed on a display screen of the user terminal 100 and connection between the user terminal 100 and the authentication server 200 is cut off.

When the user sees the service access authorization message displayed on a display screen of the user terminal 100 and inputs to the user

terminal 100 a service request to a desired service server (12), the service request is sent first from the authentication unit to the browser and then from the browser to the service server 300 via the Internet (13) (14). When the service server 300 receives the service request, a specified interface module (NSAPI), to which the service request was input, issues an authentication information request (15) (16). The authentication request is sent back from the service server 300 to the user terminal 100 via the Internet (17).